WOJSKOWA AKADEMIA TECHNICZNA

WYDZIAŁ CYBERNETYKI

CLUSTERING-BASED METHOD FOR BOTNET DETECTION

Streszczenie

mgr inż. Hubert Ostap

Promotor: dr hab. inż. Ryszard Antkiewicz

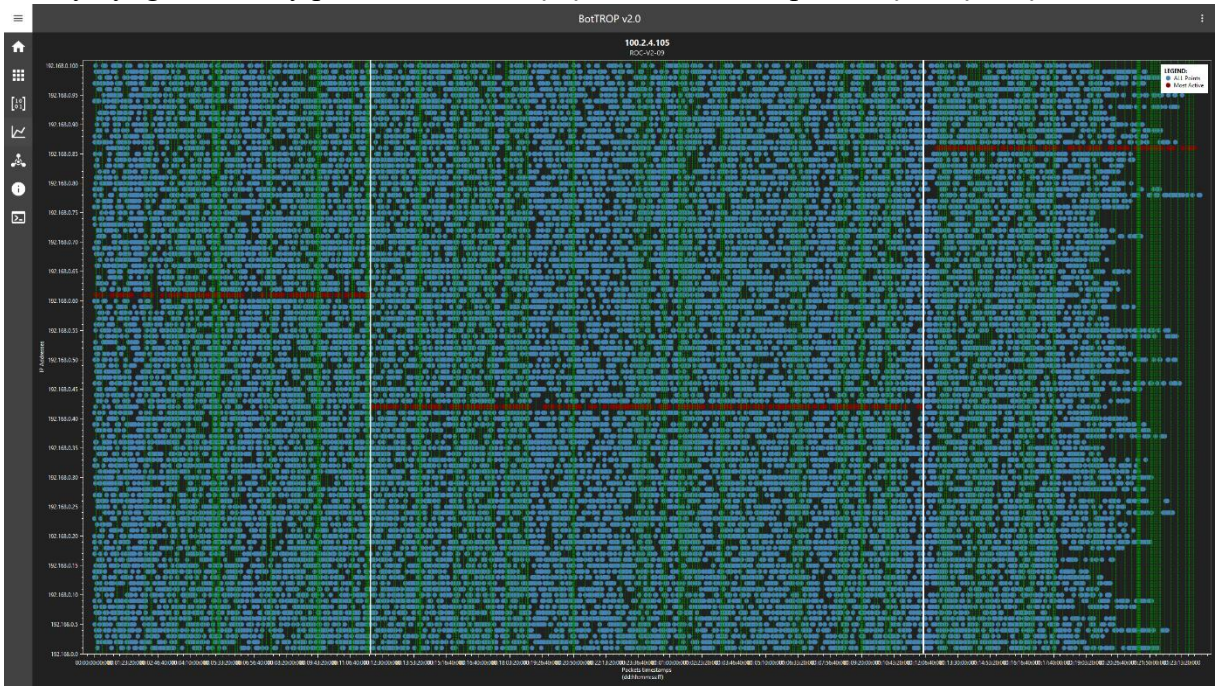
20.09.2019

Trwający wyścig zbrojeń między twórcami botnetów a twórcami metod ich wykrywania zmienił prosty, scentralizowany botnet w bardzo trudną do wykrycia hybrydową formę tego rodzaju zagrożenia. Co więcej, ciągły proces rozwoju i bardzo szybka ewolucja sprawiają, że botnety są jednymi z największych zagrożeń w cyberprzestrzeni. Ze względu na dużą liczbę ich różnych wariantów istnieje również wiele metod ich wykrywania. Z drugiej strony duży wzrost liczby nowych implementacji botnetów nie oznacza, że wszystkie metody wykrywania są rozwijane w równie szybkim tempie.

Najbardziej skuteczne metody oparte są na analizie ruchu sieciowego, które nie wymagają analizowania zawartości pakietów. Metody te nie wymagają również fizycznego dostępu do potencjalnie zainfekowanych urządzeń i są wykorzystywane do identyfikacji podejrzanej komunikacji również w zaszyfrowanym ruchu sieciowym. Jest to główny powód, dla którego metody z tej grupy są najczęściej rozwijane. Swoją popularność zawdzięczają m.in. prostocie użytkowania. W większości przypadków nie wymagają dodatkowego sprzętu; ponadto ich użytkowanie nie wymaga modyfikacji struktury sieci. Dopiero po bezinwazyjnym zidentyfikowaniu podejrzanej komunikacji oraz urządzeń, które ten ruch generują może nastąpić empiryczne sprowadzenie czy analizowane urządzenie jest częścią botnetu. Opisywane metody mogą zostać wykorzystane w dowolnej części cyklu życia botnetu, ale ich główną zaletą jest możliwość wykrycia nawet nieznanych botnetów w fazie tworzenia lub utrzymania, które do tej pory nie zostały wykorzystywane do żadnego ataku. Istnieje podgrupa szczególnie skutecznych metod opartych na wykrywaniu działania synchronicznego (aktywności grupowej), jej reprezentantem jest metoda BotGAD. Jej wysoka wydajność opiera się na założeniu, że botnety - aby osiągnąć swoje cele - muszą działać synchronicznie. W celu przeprowadzenia udanej kampanii SPAM lub ataku DDoS, Botmaster musi użyć jak największej liczby botów. Podczas badań zaobserwowano, że aktywność synchroniczna występuje nie tylko w fazie ataku, ale także w fazie tworzenia i zarządzania botnetem. Ten fakt pozwala nam wykryć zagrożenie przed pierwszym atakiem, co stanowi dużą poprawę w porównaniu z już znanymi metodami.

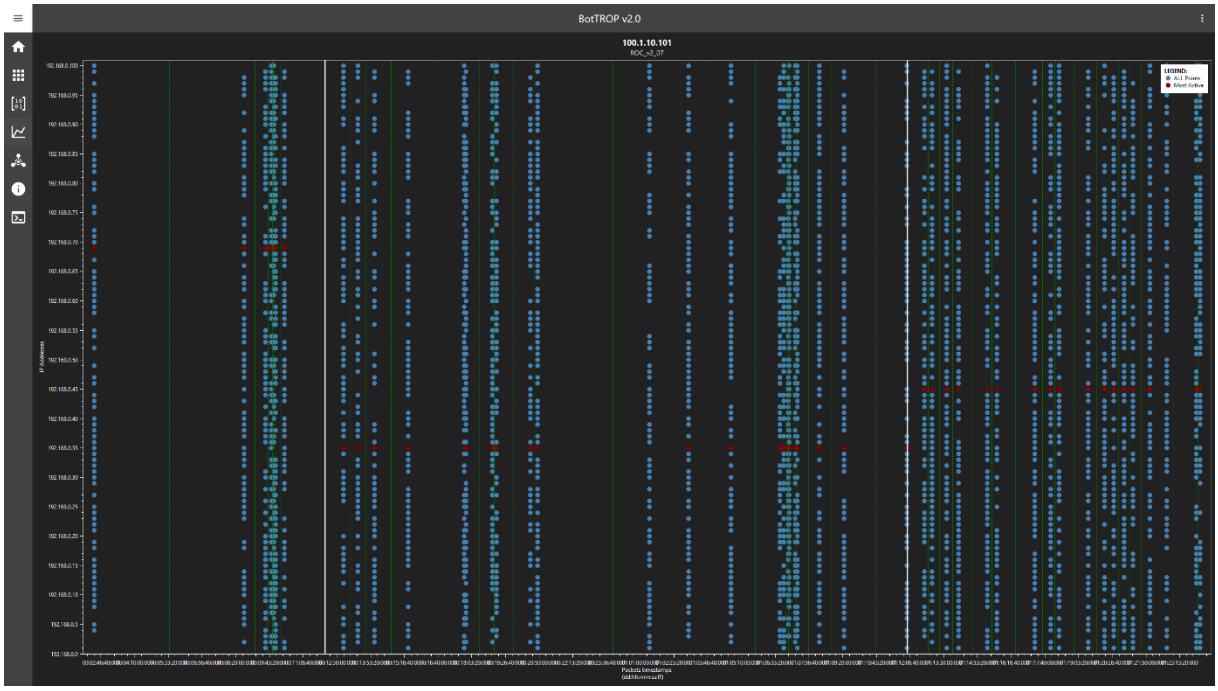
Podczas badań nad różnymi metodami wykrywania botnetów (zwłaszcza BotGAD) zaobserwowano również sytuacje, w których legalni użytkownicy generują ruch synchroniczny, na przykład z wykorzystaniem serwisów internetowych jak Facebook lub Twitter podczas bardzo popularnych wydarzeń, takich jak mistrzostwa świata w piłce nożnej lub znaczące wydarzenia polityczne. Wszystkie posty i komentarze pisane podczas takich zdarzeń są generowane z dużą intensywnością, dlatego ten rodzaj ruchu sieciowego może być rozpoznawany jako działanie synchroniczne. Mimo to nawet w takich sytuacjach współczynnik podobieństwa cosinusowego nigdy nie przekracza poziomu 0,5. Rysunek Rys.1 przedstawia graficzną reprezentację takiej sytuacji. Każdy źródłowy adres IP, który łączy się z analizowanym docelowym adresem IP, jest umieszczony na osi pionowej, a momenty, w których miało miejsce to połączenie, znajdują się na osi poziomej. Czerwone kropki oznaczają czas połączenia, który należy do najbardziej aktywnego źródłowego adresu IP. Pomiędzy każdą parą czerwonych kropek znajduje się zielona pionowa linia, jest to granica między klastrami; Niebieskie kropki oznaczają połączenia źródłowych adresów IP, które

znajdują się w wybranej sieci korporacyjnej, z analizowanym docelowym adresem IP. Jeśli ruch sieciowy był gromadzony przez kilka dni, będą one oddzielone pionową białą linią.



Rys. 1 Legalny ruch sieciowy, którego współczynnik podobieństwa cosinusowego wynosi 0.5.

Podczas badań, nawet intensywniejszy legalny ruch sieciowy nigdy nie przekroczył wartości 0,5. Dla porównania, typowe zachowanie synchroniczne botneta przedstawia rysunek Rys. 2:



Rys. 2 Synchroniczny ruch sieciowy wygenerowany przez botnet.

Graficzna reprezentacja zamieszczona powyżej przedstawia znacznie rzadszy ruch sieciowy, ale jego specyficzne wygenerowanie powoduje, że współczynnik podobieństwa cosinusowego jest bardzo wysoki (0,8). Porównanie to potwierdza skuteczność metody

BotTROP nawet podczas bardzo intensywnego ruchu sieciowego generowanego przez legalnych użytkowników oraz botnety.

Istnieje wiele różnych metod wykrywania botnetów, ale większość z nich nie jest skuteczna przeciwko nieznanym zagrożeniom, ponadto większość z nich umożliwia wykrycie botnetu, który wykorzystuje tylko jeden określony protokół. Algorytm opisany w niniejszej rozprawie jest próbą zmiany tej sytuacji i zwiększenia bezpieczeństwa sieci. BotTROP, podobnie jak BotGAD, identyfikuje nie tylko dobrze znane botnety (co udowodniono w eksperymentach z Powershell Empire, Neris i innymi), ale także nieznane zagrożenia (na przykład TwitterBot oparty na sieciach społecznościowych, który został zaimplementowany na potrzeby tej rozprawy). Ponadto, metoda BoTROP posiada ulepszony algorytm wykrywania aktywności synchronicznej występującej w różnych protokołach sieciowych.

Zadaniem naukowym niniejszej rozprawy było zbudowanie metody wykrywania botnetów poprzez identyfikację aktywności synchronicznej, tak aby spełnione były następujące wymagania:

- do wykrycia komunikacji synchronicznej zastosowana zostanie metoda klasteryzacji ruchu sieciowego;
- możliwa będzie analiza ruchu sieciowego dla dowolnego protokołu komunikacyjnego;
- możliwe będzie wykrycie nie tylko znanych botnetów, ale także tych wcześniej niezidentyfikowanych;
- skuteczność wykrywania botnetów będzie wyższa niż w przypadku wcześniej znanych metod opartych na identyfikacji komunikacji synchronicznej.

Metoda BotTROP stanowi modyfikację algorytmu BotGAD, której najważniejsze ulepszenia i zmiany zostały wymienione poniżej:

- zrezygnowano z grupowania ruchu w ramach ściśle określonego okna czasowego; zamiast tego wykorzystana została metoda klasteryzacji grup momentów, w których komunikacja z określonym docelowym adresem IP jest powtarzana (lub z grupą takich adresów). Ta procedura pozwala nam usunąć podstawową wadę BotGAD, tj. potrzebę określenia wielkości okna czasowego. Prawidłowe określenie długość tego parametru ma znaczący wpływ na skuteczność tej metody;
- umożliwiono analizę wielu różnych protokołów komunikacyjnych;
- przyspieszony został proces analizy, co jest szczególnie ważne w rozległych sieciach teleinformatycznych;
- zakładając synchroniczną aktywność botnetów, możliwe było ich wykrycie podczas fazy tworzenia i utrzymania przed przeprowadzeniem pierwszego ataku. Dzięki zaproponowanej metodzie możliwe jest nie tylko zidentyfikowanie C2, ale także wszystkich zainfekowanych urządzeń należących do zidentyfikowanego botnetu w monitorowanej sieci korporacyjnej.

Ważną częścią niniejszej rozprawy była weryfikacja właściwości metody BotTROP. Podczas tego procesu napotkano następujące problemy:

- bardzo niska dostępność ruchu sieciowego generowanego przez prawdziwe botnety. Wyjątkiem jest złośliwy ruch sieciowy udostępniony przez naukowców z Czeskiego Uniwersytetu Technicznego, który został zebrany przez Honeypot uruchomiony w ramach projektu Malware Capture Facility Project. Ponadto do weryfikacji wykorzystano ruch sieciowy Wojskowej Akademii Technicznej. Oprócz legalnego ruchu zidentyfikowano w nim 12 adresów IP powiązanych z różnymi botnetami, które

zostały pomyślnie zidentyfikowane przez BotTROP oraz usługi sieciowe monitorującego tego typu zagrożenia (VirusTotal, HybridAnalysis, GoogleSafeBrowsing). Ponadto, w zgromadzonym ruchu zidentyfikowano 36 adresów IP, z którymi komunikacja była prowadzona w sposób szczególnie synchroniczny, fakt ten może wskazywać, że są one również powiązane z sieciami botnet. Adresy te nie zostały zidentyfikowane jako C2 przez inne metody wykrywające botnety;

- ruch sieciowy generowany przez nieznane botnety nie jest dostępny z oczywistych powodów. Aby zweryfikować zdolność BotTROPa do wykrywania niezidentyfikowanych botnetów, zaimplementowano dwa symulatory: Legal Network Traffic Simulator (LNTS) i Botnet Network Traffic Simulator (BNTS). Ponadto, w tym celu dokonano implementacji narzędzia TwitterBOT.

Algorytm BotTROP, którego wymagania zostały przedstawione powyżej, został w pełni zaimplementowany i przetestowany zarówno w ruchu symulowanym, jak i w rzeczywistym. W celu porównania go z inną metodą zaimplementowano algorytm BotGAD, który podobnie jak BotTROP, próbuje wykryć aktywność synchroniczną. Dzięki temu możliwe było empiryczne porównanie, które wykazało znaczną przewagę metody BotTROP. Warto dodać, że metoda BotGAD została zaimplementowana przez jej twórców tylko na potrzeby protokołu DNS. Dla celów porównawczych autor rozprawy rozszerzył jej funkcjonalność na cały ruch TCP i UDP.

Weryfikacja metody BotTROP wymagała przeprowadzenia dwóch rodzajów różnych eksperymentów:

1. Eksperyment, którego celem jest wykrycie prawdziwych i symulowanych botnetów na podstawie ruchu sieciowego złożonego z następujących elementów:
   - rzeczywisty ruch sieci komputerowej Wojskowej Akademii Technicznej w Warszawie;
   - ruch sieciowy generowany przez rzeczywiste złośliwe oprogramowanie, zarejestrowany na Czeskim Uniwersytecie Technicznym w Pradze podczas w ramach projektu Malware Capture Facility Project (MCFP);
   - ruch sieciowy generowany przez Powershell Empire i TwitterBot;
2. Eksperyment, którego celem jest wykrycie botnetów w ruchu sieciowym generowanym przez symulator botnetu oraz symulator ruchu legalnego.

Celem pierwszego eksperymentu była weryfikacja zdolności metody BotTROP do wykrywania znanych i nieznanych botnetów w trakcie analizy dowolnego protokołu komunikacyjnego - wyniki przedstawiono w rozdziale 5.1. Drugi eksperyment miał na celu ocenę jakości metody BotTROP i porównanie jej z jakością metody BotGAD - wyniki przedstawiono w rozdziale 5.2. Otrzymane rezultaty dowodzą, że BotTROP jest wydajną metodą wykrywania wszelkiego rodzaju botnetów, niezależnie od wykorzystywanego protokołu i architektury. Bardzo ważne jest podkreślenie, iż rolą metody BotTROP jest identyfikacja aktywności synchronicznej, która w większości przypadków wiąże się ze aktywnością złośliwą. Wykorzystanie białej listy, która zawierać będzie znane publiczne adresy IP, które charakteryzują się aktywnością synchroniczna, na przykład podczas aktualizacji systemu lub sygnatur programów antywirusowych, może pomóc w zmniejszeniu liczby False Positives oraz False Negatives. Przedstawione wyniki pokazują również, że metoda BotGAD jest bardzo zależna od parametru okna czasowego, co jest jedną z jej największych wad. Powyższe sprawia, że metoda ta nie może zostać wykorzystana do wykrycia nieznanych

botnetów, ponieważ konieczne jest ustawienie odpowiedniego parametru dla sesji komunikacyjnych pomiędzy botami i ich C2 co w przypadku nieznanych zagrożeń jest niemożliwe. Metoda BotTROP jest niezależna od parametrów okna czasowego i może być skutecznie stosowana nawet w przypadku nieznanego, złośliwego lub legalnego ruchu sieciowego, co z kolei umożliwia identyfikację nieznanego botnetu.

Możliwe jest wykorzystanie metody BotTROP w środowisku produkcyjnym w obecnej formie. W tym celu konieczne jest jedynie udostępnienie ruchu sieciowego do analizy. Obecnie odbywa się to poprzez zapisanie ruchu w osobnym pliku. Następnie jest on analizowany przez algorytm BotTROP, administrator ma możliwość weryfikacji podobieństwa cosinusowego dla każdego adresu docelowego wraz z wynikami metody SPRT. Opisane narzędzie zostało rozszerzone o możliwość ciągłego monitorowania i obliczania uzyskanych wyników w celu przekształcenia ich w wykres pokazujący zależność podobieństwa cosinusowego i czasu. Umożliwi to administratorowi wizualne obserwowanie kolejnych zmian i szybką identyfikację ruchu synchronicznego, który może pojawić się lub zniknąć w zależności od dnia tygodnia. Funkcja ta jest szczególnie przydatna wobec botnetów, które mają zmienną aktywność (np. nie są aktywne w określonych dniach). Analizując ruch sieciowy w Wojskowej Akademii Technicznej, zaobserwowano, że średnie podobieństwo cosinusowe zmniejszyło się w weekend, zjawisko to było spowodowane regularnym wyłączeniem sprzętu komputerowego w tych dniach.

Wytworzone narzędzie spełnia wszystkie wymagania postawione w ramach zdefiniowanego zadania naukowego, jednocześnie wykazując bardzo wysoką skuteczność nie tylko w symulowanym ruchu, ale także w ramach rzeczywistej komunikacji pomiędzy botami i C2.

Aktualnie trwają prace nad możliwością analizy on-line bez konieczności zbierania analizowanego ruchu sieciowego. Ponadto, w najbliższej przyszłości planowane jest wprowadzenie wielu innych ulepszeń.